

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2002-279198
(P2002-279198A)

(43)公開日 平成14年9月27日(2002.9.27)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード(参考)
G 0 6 F 17/60	2 4 8	G 0 6 F 17/60	2 4 8 3 E 0 4 0
G 0 7 D 9/00	4 3 6	G 0 7 D 9/00	4 3 6 A

審査請求 有 請求項の数18 O L (全 16 頁)

(21)出願番号 特願2001-74578(P2001-74578)
(22)出願日 平成13年3月15日(2001.3.15)

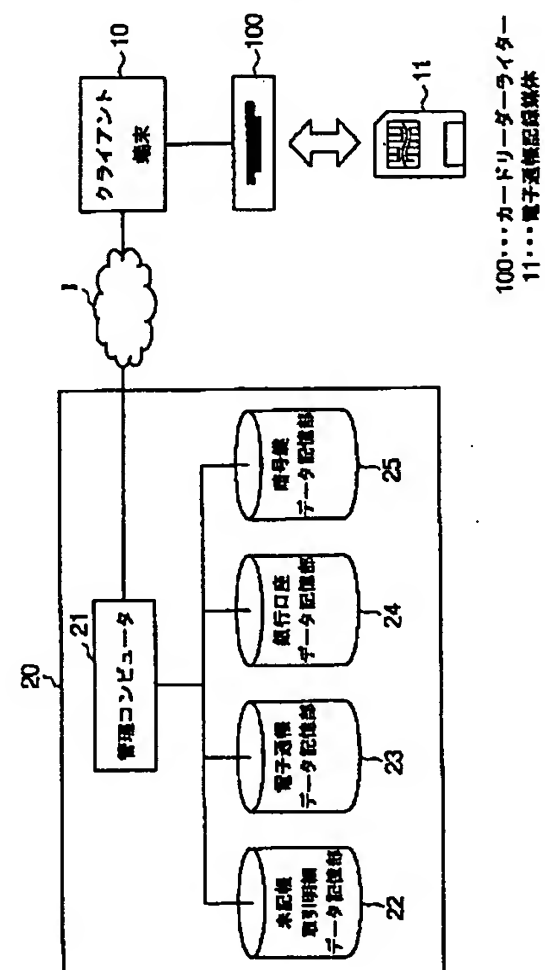
(71)出願人 592052416
株式会社みずほコーポレート銀行
東京都千代田区丸の内1丁目3番3号
(72)発明者 藤本 真紀子
東京都千代田区大手町1丁目5番5号 株
式会社富士銀行内
(74)代理人 100068755
弁理士 恩田 博宜 (外1名)
Fターム(参考) 3E040 AA07 BA01 BA06 BA16 BA18
CA12 CB10 DA10 EA02 EA10
FK08

(54)【発明の名称】 電子通帳記録方法、電子通帳登録システム及びコンピュータ読み取り可能な電子通帳記録媒体

(57)【要約】

【課題】 利用者にとって効率的であり、金融機関にとっても確実に取引明細データを記録した電子通帳を提供することができる電子通帳記録方法、電子通帳登録システム及び電子通帳記録媒体を提供することにある。

【解決手段】 利用者は、クライアント端末10を用いてユーザ認証を行った後で、電子通帳記録媒体11に記録された媒体識別子121を電子通帳登録システム20に送信する。管理コンピュータ21は、受信した媒体識別子121と銀行口座に関するデータとから通帳識別子を生成する。さらに、管理コンピュータ21は、この通帳識別子を銀行秘密鍵251で暗号化し、銀行署名データを生成する。そして、管理コンピュータ21は、クライアント端末10に通帳識別子と銀行署名データとを送信する。クライアント端末10はこれらのデータを電子通帳記録媒体11に記録する。これによって、銀行に認証された電子通帳記録媒体11が生成される。



【特許請求の範囲】

【請求項1】 管理コンピュータを有する電子通帳登録システムを用いて、金融機関における取引明細データを記録媒体に記録する電子通帳記録方法であって、前記管理コンピュータが、前記記録媒体のデータ書込み不可領域から抽出した媒体識別子を受信し、電子通帳データ記憶手段に記録する第1の段階と、前記管理コンピュータが、前記媒体識別子に基づいて金融機関秘密鍵で暗号化した金融機関署名データを生成する第2の段階と、前記管理コンピュータが、前記金融機関署名データを前記記録媒体に記録するために出力する第3の段階とを有することを特徴とする電子通帳記録方法。

【請求項2】 前記電子通帳記録方法は、前記管理コンピュータが、前記媒体識別子と金融機関口座識別子とに基づいて通帳識別子を生成し、前記電子通帳データ記憶手段に記録する段階をさらに有し、前記第2の段階は、前記通帳識別子を前記金融機関秘密鍵で暗号化して金融機関署名データを生成し、前記第3の段階は、前記通帳識別子と前記金融機関署名データとを前記記録媒体に記録するために出力することを特徴とする請求項1に記載の電子通帳記録方法。

【請求項3】 前記電子通帳記録方法は、前記取引明細データを送信する場合には、前記管理コンピュータが、前記記録媒体から前記媒体識別子、前記通帳識別子の少なくとも一方に関するデータを受信し、前記電子通帳データ記憶手段に記録されたデータと照合する段階と、認証ができた場合には、前記管理コンピュータが前記記録媒体に記録する取引明細データを抽出する段階と、前記管理コンピュータが、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化し、前記記録媒体に記録するために出力する段階とをさらに有することを特徴とする請求項1又は2に記載の電子通帳記録方法。

【請求項4】 前記電子通帳記録方法は、前記管理コンピュータが、一方向関数を用いて前記取引明細データの一方向関数計算値を算出する段階と、前記取引明細データを送信する場合には、前記管理コンピュータが、前記一方向関数計算値に関するデータを、前記記録媒体に記録するために出力する段階とをさらに有することを特徴とする請求項1～3のいずれか1項に記載の電子通帳記録方法。

【請求項5】 前記一方向関数計算値に関するデータは、前記媒体識別子に関連するデータを用いて、前記一方向関数計算値を暗号化したデータであることを特徴とする請求項1～4のいずれか1項に記載の電子通帳記録方法。

【請求項6】 前記電子通帳記録方法は、前記管理コンピュータが、既に前記記録媒体に記録され

た取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから、新しい一方向関数計算値を生成し、記録する段階をさらに有することを特徴とする請求項4又は5に記載の電子通帳記録方法。

【請求項7】 金融機関における取引明細データを記録媒体に記録するための電子通帳登録システムであって、前記記録媒体のデータ書込み不可領域から抽出した媒体識別子を記録する電子通帳データ記憶手段と、前記金融機関の金融機関秘密鍵に関するデータを記録した暗号鍵データ記憶手段と、前記媒体識別子に基づいて前記金融機関秘密鍵で暗号化した金融機関署名データを生成し、前記記録媒体に記録するために前記金融機関署名データを出力する管理コンピュータとを有することを特徴とする電子通帳登録システム。

【請求項8】 前記電子通帳登録システムは、金融機関口座識別子を記録する金融機関口座データ記憶手段をさらに有し、前記管理コンピュータは、前記媒体識別子と前記金融機関口座識別子とに基づいて通帳識別子を生成し、前記通帳識別子を前記金融機関秘密鍵で暗号化して金融機関署名データを生成し、前記通帳識別子と前記金融機関署名データとを前記記録媒体に記録するために出力することを特徴とする請求項7に記載の電子通帳登録システム。

【請求項9】 前記管理コンピュータは、前記記録媒体に記録する取引明細データを抽出し、前記取引明細データを送信する場合には、前記管理コンピュータが、前記記録媒体から前記媒体識別子、前記通帳識別子の少なくとも一方に関するデータを受信し、前記電子通帳データ記憶手段に記録されたデータと照合し、認証ができた場合には、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化し、前記記録媒体に記録するために出力することを特徴とする請求項7又は8に記載の電子通帳登録システム。

【請求項10】 前記管理コンピュータは、一方向関数を用いて、前記取引明細データの一方向関数計算値を算出し、前記取引明細データを送信する場合には、前記管理コンピュータが、前記一方向関数計算値に関するデータを、前記記録媒体に記録するために出力することを特徴とする請求項7～9のいずれか1項に記載の電子通帳登録システム。

【請求項11】 前記一方向関数計算値に関するデータは、前記一方向関数計算値を、前記媒体識別子に関連するデータを用いて暗号化したデータであることを特徴とする請求項7～10のいずれか1項に記載の電子通帳登録システム。

【請求項１２】 前記管理コンピュータは、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから、新しい一方向関数計算値を生成し、前記電子通帳データ記憶手段に、前記生成した一方向関数計算値をさらに記録することを特徴とする請求項１０又は１１に記載の電子通帳登録システム。

【請求項１３】 金融機関における取引明細データを記録するための電子通帳記録媒体であって、前記電子通帳記録媒体が、前記電子通帳記録媒体の媒体識別子を記録したデータ書込み不可領域と、データ書込み可能領域とを有し、前記データ書込み可能領域には、前記媒体識別子に関するデータを金融機関秘密鍵で暗号化した金融機関署名データを記録したことを特徴とするコンピュータ読み取り可能な電子通帳記録媒体。

【請求項１４】 前記データ書込み可能領域には、前記媒体識別子と金融機関口座識別子とに基づいて生成された通帳識別子をさらに記録したことを特徴とする請求項１３に記載のコンピュータ読み取り可能な電子通帳記録媒体。

【請求項１５】 前記データ書込み可能領域には、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化したデータをさらに記録したことを特徴とする請求項１３又は１４に記載のコンピュータ読み取り可能な電子通帳記録媒体。

【請求項１６】 前記データ書込み可能領域には、一方向関数を用いて算出した前記取引明細データの一方方向関数計算値に関するデータをさらに記録したことを特徴とする請求項１３～１５のいずれか１項に記載のコンピュータ読み取り可能な電子通帳記録媒体。

【請求項１７】 前記一方向関数計算値に関するデータは、前記一方向関数計算値を前記媒体識別子に関連するデータを用いて暗号化したデータであることを特徴とする請求項１３～１６のいずれか１項に記載のコンピュータ読み取り可能な電子通帳記録媒体。

【請求項１８】 前記データ書込み可能領域には、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから生成された一方向関数計算値がさらに記録されていることを特徴とする請求項１６又は１７に記載のコンピュータ読み取り可能な電子通帳記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】 本発明は、銀行口座の利用履歴に関する取引明細データの記録に用いる電子通帳記録方法、電子通帳登録システム及びコンピュータ読み取り可能な電子通帳記録媒体に関するものである。

【０００２】

【従来の技術】 今日、資金を受け取る場合には、金融機関の提供するバンキングサービスを利用して、利用者自身の金融機関口座（例えば、銀行口座）に資金を振り込んでもらうことがある。また、利用者自身も、自身の金融機関口座の資金を他人の金融機関口座に振り込んだりする。一方、現金が必要な場合、利用者自身の金融機関口座から現金を引き出したりする場合もある。このような場合、キャッシュカードを利用して、現金自動預け払い機（ＡＴＭ：Automatic Teller Machine）または現金支払機（ＣＤ：Cash Dispenser）を用いる場合がある。一方、金融機関口座の通帳（例えば、預金通帳）を使用せずに行われた取引明細に関するデータ（未記帳取引明細データ）は、金融機関のシステムに保存されており、金融機関が付与した預金通帳が利用された際にまとめて処理される。具体的には、金融機関口座における取引の内容（取引明細）は、通帳記帳の可能な端末において、その預金通帳に印刷される。このような場合、この預金通帳は、利用者の金融機関に対する預金債権の存在を確認する性格を有するものである。

【０００３】

【発明が解決しようとする課題】 しかし、利用者が預金通帳に取引明細を記帳するためには、ＡＴＭや通帳記帳端末等の設置された金融機関の店舗に出向く必要がある。このため、利用者は、迅速に取引状況、現在残高を把握することができなかった。一方、利用者のコンピュータ端末等を用い、電話回線やインターネット等のネットワークを介して金融機関の提供するバンキングサービスを利用して、預金残高照会を行うこともできる。しかし、この預金残高照会結果を印刷しても、預金債権の存在を確認するものとはならない。

【０００４】 本発明は、上記問題点を解決するためになされたものであり、その目的は、利用者にとって効率的であり、金融機関にとっても確実に取引明細データを記録した電子通帳を提供することができる電子通帳記録方法、電子通帳登録システム及びコンピュータ読み取り可能な電子通帳記録媒体を提供することにある。

【０００５】

【課題を解決するための手段】 上記問題点を解決するために、請求項１に記載の発明は、管理コンピュータを有する電子通帳登録システムを用いて、金融機関における取引明細データを記録媒体に記録する電子通帳記録方法であって、前記管理コンピュータが、前記記録媒体のデータ書込み不可領域から抽出した媒体識別子を受信し、電子通帳データ記憶手段に記録する第１の段階と、前記管理コンピュータが、前記媒体識別子に基づいて金融機関秘密鍵で暗号化した金融機関署名データを生成する第２の段階と、前記管理コンピュータが、前記金融機関署名データを前記記録媒体に記録するために出力する第３の段階とを有することを要旨とする。

【０００６】 請求項２に記載の発明は、請求項１に記載

の電子通帳記録方法において、前記電子通帳記録方法は、前記管理コンピュータが、前記媒体識別子と金融機関口座識別子とに基づいて通帳識別子を生成し、前記電子通帳データ記憶手段に記録する段階をさらに有し、前記第2の段階は、前記通帳識別子を前記金融機関秘密鍵で暗号化して金融機関署名データを生成し、前記第3の段階は、前記通帳識別子と前記金融機関署名データとを前記記録媒体に記録するために出力することを要旨とする。

【0007】請求項3に記載の発明は、請求項1又は2に記載の電子通帳記録方法において、前記電子通帳記録方法は、前記取引明細データを送信する場合には、前記管理コンピュータが、前記記録媒体から前記媒体識別子、前記通帳識別子の少なくとも一方に関するデータを受信し、前記電子通帳データ記憶手段に記録されたデータと照合する段階と、認証ができた場合には、前記管理コンピュータが前記記録媒体に記録する取引明細データを抽出する段階と、前記管理コンピュータが、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化し、前記記録媒体に記録するために出力する段階とをさらに有することを要旨とする。

【0008】請求項4に記載の発明は、請求項1～3のいずれか1項に記載の電子通帳記録方法において、前記電子通帳記録方法は、前記管理コンピュータが、一方向関数を用いて前記取引明細データの一方向関数計算値を算出する段階と、前記取引明細データを送信する場合には、前記管理コンピュータが、前記一方向関数計算値に関するデータを、前記記録媒体に記録するために出力する段階とをさらに有することを要旨とする。

【0009】請求項5に記載の発明は、請求項1～4のいずれか1項に記載の電子通帳記録方法において、前記一方向関数計算値に関するデータは、前記媒体識別子に関連するデータを用いて、前記一方向関数計算値を暗号化したデータであることを要旨とする。

【0010】請求項6に記載の発明は、請求項4又は5に記載の電子通帳記録方法において、前記電子通帳記録方法は、前記管理コンピュータが、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから、新しい一方向関数計算値を生成し、記録する段階をさらに有することを要旨とする。

【0011】請求項7に記載の発明は、金融機関における取引明細データを記録媒体に記録するための電子通帳登録システムであって、前記記録媒体のデータ書込み不可領域から抽出した媒体識別子を記録する電子通帳データ記憶手段と、前記金融機関の金融機関秘密鍵に関するデータを記録した暗号鍵データ記憶手段と、前記媒体識別子に基づいて前記金融機関秘密鍵で暗号化した金融機関署名データを生成し、前記記録媒体に記録するために前記金融機関署名データを出力する管理コンピュータと

を有することを要旨とする。

【0012】請求項8に記載の発明は、請求項7に記載の電子通帳登録システムにおいて、前記電子通帳登録システムは、金融機関口座識別子を記録する金融機関口座データ記憶手段をさらに有し、前記管理コンピュータは、前記媒体識別子と前記金融機関口座識別子とに基づいて通帳識別子を生成し、前記通帳識別子を前記金融機関秘密鍵で暗号化して金融機関署名データを生成し、前記通帳識別子と前記金融機関署名データとを前記記録媒体に記録するために出力することを要旨とする。

【0013】請求項9に記載の発明は、請求項7又は8に記載の電子通帳登録システムにおいて、前記管理コンピュータは、前記記録媒体に記録する取引明細データを抽出し、前記取引明細データを送信する場合には、前記管理コンピュータが、前記記録媒体から前記媒体識別子、前記通帳識別子の少なくとも一方に関するデータを受信し、前記電子通帳データ記憶手段に記録されたデータと照合し、認証ができた場合には、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化し、前記記録媒体に記録するために出力することを要旨とする。

【0014】請求項10に記載の発明は、請求項7～9のいずれか1項に記載の電子通帳登録システムにおいて、前記管理コンピュータは、一方向関数を用いて、前記取引明細データの一方向関数計算値を算出し、前記取引明細データを送信する場合には、前記管理コンピュータが、前記一方向関数計算値に関するデータを、前記記録媒体に記録するために出力することを要旨とする。

【0015】請求項11に記載の発明は、請求項7～10のいずれか1項に記載の電子通帳登録システムにおいて、前記一方向関数計算値に関するデータは、前記一方向関数計算値を、前記媒体識別子に関連するデータを用いて暗号化したデータであることを要旨とする。

【0016】請求項12に記載の発明は、請求項10又は11に記載の電子通帳登録システムにおいて、前記管理コンピュータは、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから、新しい一方向関数計算値を生成し、前記電子通帳データ記憶手段に、前記生成した一方向関数計算値をさらに記録することを要旨とする。

【0017】請求項13に記載の発明は、金融機関における取引明細データを記録するための電子通帳記録媒体であって、前記電子通帳記録媒体が、前記電子通帳記録媒体の媒体識別子を記録したデータ書込み不可領域と、データ書込み可能領域とを有し、前記データ書込み可能領域には、前記媒体識別子に関するデータを金融機関秘密鍵で暗号化した金融機関署名データを記録したことを要旨とする。

【0018】請求項14に記載の発明は、請求項13に

記載のコンピュータ読み取り可能な電子通帳記録媒体において、前記データ書込み可能領域には、前記媒体識別子と金融機関口座識別子とに基づいて生成された通帳識別子をさらに記録したことを要旨とする。

【0019】請求項15に記載の発明は、請求項13又は14に記載のコンピュータ読み取り可能な電子通帳記録媒体において、前記データ書込み可能領域には、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化したデータをさらに記録したことを要旨とする。

【0020】請求項16に記載の発明は、請求項13～15のいずれか1項に記載のコンピュータ読み取り可能な電子通帳記録媒体において、前記データ書込み可能領域には、一方向関数を用いて算出した前記取引明細データの一方向関数計算値に関するデータをさらに記録したことを要旨とする。

【0021】請求項17に記載の発明は、請求項13～16のいずれか1項に記載のコンピュータ読み取り可能な電子通帳記録媒体において、前記一方向関数計算値に関するデータは、前記一方向関数計算値を前記媒体識別子に関連するデータを用いて暗号化したデータであることを要旨とする。

【0022】請求項18に記載の発明は、請求項16又は17に記載のコンピュータ読み取り可能な電子通帳記録媒体において、前記データ書込み可能領域には、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから生成された一方向関数計算値がさらに記録されていることを要旨とする。

【0023】（作用）請求項1又は7に記載の発明によれば、管理コンピュータが、媒体識別子に基づいて金融機関秘密鍵で暗号化した金融機関署名データを生成し、この金融機関署名データを記録媒体に記録するために出力する。このため、この記録媒体を金融機関の提供する電子通帳として利用できる。

【0024】請求項2又は8に記載の発明によれば、管理コンピュータが、媒体識別子と金融機関口座識別子とに基づいて生成した通帳識別子を金融機関秘密鍵で暗号化して金融機関署名データを生成する。このため、金融機関署名データには、金融機関口座識別子に関するデータが含まれる。従って、一つの記録媒体の中に、複数の金融機関口座に関する通帳を生成できる。

【0025】請求項3又は9に記載の発明によれば、管理コンピュータが、記録媒体から媒体識別子、通帳識別子の少なくとも一方に関するデータを受信し、受信したデータと電子通帳データ記憶手段に記録されたデータと照合し、認証できれば取引明細に関するデータを送信する。このため、金融機関によって認証されていない記録媒体への取引明細に関するデータの記録を防止できる。また、管理コンピュータは、取引明細データを媒体識別

子に関連するデータを用いて暗号化し、記録媒体に記録するために出力する。このため、取引明細データを記録媒体と関連づけて記録できる。従って、取引明細データを、予め定められた記録媒体に安全、確実に記録できる。

【0026】請求項4又は10に記載の発明によれば、管理コンピュータが、一方向関数を用いて取引明細データの一方向関数計算値を算出し、記録媒体に記録するために、この一方向関数計算値に関するデータを出力する。このため、記録媒体に記録された取引明細データと一方向関数計算値とから、取引明細データの真正性を担保することができる。

【0027】請求項5又は11に記載の発明によれば、一方向関数計算値に関するデータは、前記媒体識別子に関連するデータを用いて、前記一方向関数計算値を暗号化したデータである。このため、取引明細データは媒体識別子と関連づけられ、電子通帳の唯一性を担保できる。

【0028】請求項6又は12に記載の発明によれば、管理コンピュータが、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから、新しい一方向関数計算値を生成し、記録する。このため、一方向関数計算値には、過去の取引明細データが含まれる。これにより、取引明細の連続性を担保でき、一部の取引明細データを削除、追加、改変した場合にも、偽造、改変を確実に把握できる。

【0029】請求項13に記載の発明によれば、電子通帳記録媒体には、記録媒体の媒体識別子を記録したデータ書込み不可領域と、媒体識別子に関するデータを金融機関秘密鍵で暗号化した金融機関署名データを記録したデータ書込み可能領域が設けられている。金融機関署名データは、データ書込み不可領域に記録された媒体識別子を用いて生成されるので、偽造、改変を防止できる。そして、金融機関署名データに基づいて、金融機関が提供する通帳であることを認証できる。

【0030】請求項14に記載の発明によれば、データ書込み可能領域には、媒体識別子と金融機関口座識別子とに基づいて生成された通帳識別子が、さらに記録されている。このため、金融機関署名データには金融機関口座識別子の情報が含まれ、一つの記録媒体に複数の金融機関口座に関する通帳を生成できる。

【0031】請求項15に記載の発明によれば、前記データ書込み可能領域に、取引明細データと、前記取引明細データを前記媒体識別子に関連するデータを用いて暗号化したデータがさらに記録されている。このため、取引明細データと媒体識別子とが関連づけられており、他の記録媒体への取引明細データの記録を防止できる。

【0032】請求項16に記載の発明によれば、前記データ書込み可能領域に、一方向関数を用いて算出した前

記取引明細データがさらに記録されている。このため、取引明細データとその一方向関数計算値とを照合することでき、取引明細データの真正性を担保することができる。

【0033】請求項17に記載の発明によれば、前記一方向関数計算値に関するデータは、前記一方向関数計算値を前記媒体識別子に関連するデータを用いて暗号化したデータである。このため、取引明細データは媒体識別子と関連づけられ、電子通帳の唯一性を担保できる。

【0034】請求項18に記載の発明によれば、前記データ書き込み可能領域には、既に前記記録媒体に記録された取引明細データに関する一方向関数計算値と、未記帳の取引明細データに関する一方向関数計算値とから生成された一方向関数計算値がさらに記録されている。このため、一方向関数計算値には、過去の取引明細データが含まれる。これにより、取引明細の連続性を担保でき、一部の取引明細データを削除、追加、改変した場合にも、偽造、改変を確実に把握できる。

【0035】

【発明の実施の形態】以下、本発明を具体化した一実施形態を図1～図10に従って説明する。本実施形態では、利用者が媒体識別子の付与された記録媒体を取得し、この記録媒体を金融機関（ここでは銀行）の取引明細データを記録する場合に用いる電子通帳記録方法、電子通帳登録システム及びコンピュータ読み取り可能な電子通帳記録媒体として説明する。この電子通帳記録媒体には、通常の預金通帳と同様に取引明細に関する情報が記録され、預金通帳としての機能を有する。

【0036】図1に示すように、取引明細に関する情報を記録する記録媒体として電子通帳記録媒体11を用いる。この電子通帳記録媒体11には、市販の記録媒体を用い、電子通帳記録媒体11に関する情報を銀行に登録し、所定のデータが記録されることにより電子通帳として機能する。

【0037】この電子通帳記録媒体11に未記帳の取引明細データを記録したり、記録された取引明細データを表示したりする場合には、利用者のクライアント端末10を用いる。クライアント端末10には、図示しないCPU、RAM、ROM等を有するコンピュータであり、各種プログラムの実行、後述するデータの管理、送受信等の制御を行う。さらに、クライアント端末10には、カードリーダーライター100が接続されている。このカードリーダーライター100に電子通帳記録媒体11を挿入し、電子通帳記録媒体11に記録されたデータをクライアント端末10に読み込んだり、電子通帳記録媒体11にデータを記録したりする。また、このクライアント端末10には、図示しないディスプレイ装置が接続されている。このディスプレイ装置を用いて、電子通帳記録媒体11に記録された取引明細を表示する。さらに、クライアント端末10には、後述するユーザ認証等

において、所定のデータを入力するためのデータ入力部が設けられている。

【0038】このクライアント端末10は、インターネットIを介して、電子通帳登録システム20に接続されている。この電子通帳登録システム20は、銀行が管理するシステムであり、電子通帳記録媒体11に関する情報、取引明細に関する情報を管理するコンピュータシステムである。また、電子通帳登録システム20は、クライアント端末10にデータを送信したり、クライアント端末10からのデータを受信したりする。

【0039】電子通帳登録システム20は、図1に示すように、管理コンピュータ21を備えている。この管理コンピュータ21は、クライアント端末10の間でデータの送受信を行う。管理コンピュータ21には、図示しないCPU、RAM、ROM等を有するコンピュータであり、各種プログラムの実行、後述するデータの管理、送受信等の制御を行う。

【0040】管理コンピュータ21には、未記帳取引明細データ記憶部22、電子通帳データ記憶手段としての電子通帳データ記憶部23、金融機関口座データ記憶手段としての銀行口座データ記憶部24、及び暗号鍵データ記憶手段としての暗号鍵データ記憶部25が、それぞれ接続されている。

【0041】以下、図2～6を用いて、電子通帳記録媒体11及び各記憶部（22～25）に記録されるデータを説明する。電子通帳記録媒体11には、図2に示すように、銀行が電子通帳記録媒体11を通帳として認証するために必要なデータが記録される。この電子通帳記録媒体11には、データ書き込み不可領域120とデータ書き込み可能領域130とが予め設定されている。このデータ書き込み不可領域120には、記録媒体を識別するための媒体固有の媒体識別子121が予め記録されている。利用者は、このデータ書き込み不可領域120に記録された媒体識別子121を変更することができない。本実施形態では、このような電子通帳記録媒体11として、データ書き込み不可領域120を有する著作権保護機能に対応したメモリーカード等を用いる。

【0042】一方、データ書き込み可能領域130には、電子通帳データ131が記録されている。この電子通帳データ131は、暗号鍵データ132、通帳識別子データ133、暗号化データ134、及び多重ハッシュ値データ135が記録されている。この暗号鍵データ132には、公開鍵暗号方式で用いる媒体秘密鍵136と媒体公開鍵137とが記録されている。この公開鍵暗号方式は、暗号化する鍵と復号化する鍵とが異なる暗号方式であって、一方を公開し、他方を秘密とする。例えば、公知のRSA（Rivest-Shamir-Adleman）方式がある。暗号鍵データ132は、電子通帳として用いる電子通帳記録媒体11を定めたときに予め記録される。

【0043】通帳識別子データ133には、通帳識別子

データと銀行署名データとが関連づけられて記録されている。この通帳識別子データ133は、利用者がこの記録媒体を電子通帳として銀行に登録の申請を行い、その申請が認められた場合に記録される。本実施形態では、この通帳識別子データ133は、通帳識別子毎に銀行署名データが記録されている。通帳識別子データ領域には、電子通帳登録システム20から付与された通帳識別子に関するデータが記録される。銀行署名データ領域には、電子通帳登録システム20で生成された銀行署名に関するデータが記録される。

【0044】暗号化データ134には、暗号化取引明細データと暗号化ハッシュ値とに関するデータとが、通帳識別子に関連づけられて記録されている。この暗号化データ134は、電子通帳登録システム20から未記帳の取引明細に関してのデータを受信する毎に追加記録される。この暗号化取引明細データ領域には、記帳する取引明細に関するデータを媒体識別子121で暗号化したデータが記録される。一方、暗号化ハッシュ値データ領域には、記帳する取引明細に関するデータのハッシュ値を媒体識別子121で暗号化したデータが記録される。ここで、ハッシュ値とは、一方向関数としての公知のハッシュ関数を用いてデータを一定の長さ（例えば、128ビット）に圧縮した一方向関数計算値である。ハッシュ関数としては、二つの異なるデータのハッシュ値が一致する確率が極めて小さい関数を用いる。

【0045】多重ハッシュ値データ135には、多重ハッシュ値に関するデータが、通帳識別子に関連づけられて記録されている。この多重ハッシュ値データ135は、その記帳する取引明細に関してのデータが真正であることが確認された場合に記録される。本実施形態では、この多重ハッシュ値データ135は、通帳識別子毎に記録されている。多重ハッシュ値データ領域には、後述するように、既に記録された取引明細に関するデータのハッシュ値と未記帳取引明細に関するデータのハッシュ値とから生成される多重ハッシュ値に関するデータが記録される。

【0046】未記帳取引明細データ記憶部22には、図3に示すように、未記帳の取引明細データ220が記録されている。この取引明細データ220は、利用者が記帳を行った後、新たに取引が行われ、記帳すべき取引明細が発生した場合に記録される。本実施形態では、取引明細データ220には、利用者の銀行口座番号と未記帳取引明細とに関するデータが関連付けられて記録されている。この銀行口座番号データ領域には、利用者が保有する銀行口座を特定するための識別子である銀行口座番号が記録される。未記帳取引明細データ領域には、利用者の電子通帳記録媒体11に記帳されていない取引明細に関するデータが記録される。この未記帳取引明細データ領域に記録されたデータは、電子通帳記録媒体11に記帳され、クライアント端末10から後述する記録完了

通知を受信した場合に消去される。

【0047】電子通帳データ記憶部23には、図4に示すように、利用者が使用する電子通帳に関する電子通帳データ230が記録される。この電子通帳データ230は、利用者から電子通帳の登録申請があった場合に生成される。本実施形態では、電子通帳データ230には、媒体識別子、通帳識別子、媒体公開鍵、最新記帳ハッシュ値、多重ハッシュ値に関するデータが、銀行口座番号に関連づけられて記録される。この媒体識別子データ領域には、利用者が電子通帳として用いる記録媒体の識別子であり、電子通帳記録媒体11のデータ書込み不可領域120に記録された媒体識別子121に関するデータが記録される。通帳識別子データ領域には、媒体識別子121と銀行口座の属性情報（識別子）に基づいて生成された通帳識別子に関するデータが記録される。媒体公開鍵データ領域には、電子通帳記録媒体11に記録された媒体公開鍵137に関するデータが記録される。この媒体公開鍵は、利用者が電子通帳の登録申請を行った場合に記録される。最新記帳ハッシュ値データ領域には、最後に電子通帳記録媒体11に記帳された取引明細に関するデータのハッシュ値に関するデータが記録される。多重ハッシュ値データ領域には、過去の多重ハッシュ値と最後に記帳された取引明細データのハッシュ値とから生成された多重ハッシュ値に関するデータが記録される。

【0048】銀行口座データ記憶部24には、図5に示すように、利用者の銀行口座に関する銀行口座データ240が記録される。この銀行口座データ240は、利用者が銀行口座を開設した場合に記録される。本実施形態では、銀行口座データ240には、金融機関口座識別子としての銀行口座番号、利用者名、暗証番号に関するデータが、利用者番号に関するデータと関連づけられて記録される。この利用者番号は、銀行が利用者を特定するために付与した識別子である。銀行口座番号データ領域には、銀行口座を特定するためのデータとして、銀行コード、支店コード、口座番号に関するデータが記録される。暗証番号データ領域には、インターネットIを介して電子通帳登録システム20にアクセスする場合に用いる本人認証のためのパスワードに関するデータが記録される。

【0049】暗号鍵データ記憶部25には、図6に示すように、クライアント端末10と電子通帳登録システム20との間で通信を行う場合に用いる銀行の暗号鍵に関する暗号鍵データ250が記録される。この暗号鍵データ250は、電子通帳登録システム20を用いて、電子通帳の登録サービスを提供するために予め設定される。本実施形態では、暗号鍵データ250には、銀行秘密鍵251、銀行公開鍵252に関するデータが記録される。これらの鍵は、暗号化を行うための鍵と復号化を行うために用いる鍵である。

【0050】次に、上記のように構成されたシステムにおいて、電子通帳を利用する場合の処理手順を図7～10に従って説明する。この場合、大きくは3つの段階からなる。すなわち、図7に示す電子通帳記録媒体11を登録する段階、図8～9に示す電子通帳登録システム20から取引明細に関するデータを記録する段階、及び図10に示す取引明細を表示する段階である。これらの段階では、利用者がクライアント端末10を用いて処理する。

【0051】まず、利用者が、クライアント端末10を用いて電子通帳記録媒体11を登録する段階の処理を、図7を用いて説明する。まず、利用者はクライアント端末10を用いてユーザ認証を行う（S1-1）。この処理は、通常のネットワークを利用したバンキング処理において行われるユーザ認証（本人認証）と同様に行われる。ここでは、まず、利用者はクライアント端末10を用いてインターネットIを介して電子通帳登録システム20にアクセスする。次に、利用者は、電子通帳登録システム20からの要求に応じて利用者番号、銀行口座番号、暗証番号に関するデータを送信する。データを受信した管理コンピュータ21は、受信した利用者番号、銀行口座番号、暗証番号が、銀行口座データ記憶部24に記録された銀行口座データ240と一致するかどうかを確認する。両者が一致する場合、管理コンピュータ21は、ユーザ認証を終了する。そして、管理コンピュータ21は、電子通帳記録媒体11の銀行が提供するサービスの利用許諾を利用者に与える。

【0052】次に、利用者は、クライアント端末10を用いて電子通帳登録要求を行う（S1-2）。この場合、クライアント端末10はインターネットIを介して、電子通帳登録要求を電子通帳登録システム20に送信する。電子通帳登録要求を受信した管理コンピュータ21は、クライアント端末10に対して媒体識別子要求と銀行公開鍵252とを送信する（S1-3）。この場合、管理コンピュータ21は、暗号鍵データ記憶部25から銀行公開鍵252を抽出し、クライアント端末10に送信する。

【0053】媒体識別子要求を受信したクライアント端末10は、利用者に対して電子通帳記録媒体11をカードリーダーライター100に挿入するように促す。具体的には、クライアント端末10のディスプレイ装置に、「電子通帳記録媒体の挿入指示」が表示される。さらに、クライアント端末10は受信した銀行公開鍵252を、図示しない記憶部に記録する。次に、電子通帳記録媒体11がカードリーダーライター100に挿入された場合、クライアント端末10は、電子通帳記録媒体11の媒体識別子121を抽出する（S1-4）。この場合、クライアント端末10は、カードリーダーライター100に挿入された電子通帳記録媒体11のデータ書込み不可領域120に記録された媒体識別子121を読み

出す。次に、クライアント端末10は、読み出した媒体識別子121を暗号化する（S1-5）。この場合の暗号化には、銀行公開鍵252を用いる。

【0054】次に、クライアント端末10は、インターネットIを介して電子通帳登録システム20に暗号化した媒体識別子121と媒体公開鍵137に関するデータを送信する（S1-6）。このデータを受信した管理コンピュータ21は、暗号化された媒体識別子121を銀行秘密鍵251で復号化し、媒体識別子を抽出する（S1-7）。そして、復号化した媒体識別子121及び媒体公開鍵137を銀行口座番号と関連付けて電子通帳データ記憶部23に記録する。

【0055】次に、管理コンピュータ21は通帳識別子を生成する（S1-8）。この場合、まず、管理コンピュータ21は銀行口座データ記憶部24から、この利用者番号に関連づけられた銀行口座に関するデータを抽出する。ここでは、銀行口座に関するデータとして、支店コードと銀行口座番号を用いる。次に、抽出した銀行口座に関するデータと媒体識別子とから通帳識別子を生成する。そして、管理コンピュータ21は生成した通帳識別子を電子通帳データ記憶部23に記録する。次に、管理コンピュータ21は、生成した通帳識別子を媒体公開鍵137で暗号化し、暗号化通帳識別子を生成する（S1-9）。さらに、管理コンピュータ21は、電子通帳データ記憶部23に記録した通帳識別子を、銀行秘密鍵251で暗号化して銀行電子署名データを生成する（S1-10）。

【0056】次に、管理コンピュータ21は、インターネットIを介して、暗号化通帳識別子及び銀行電子署名に関するデータをクライアント端末10に送信する（S1-11）。このデータを受信したクライアント端末10は、受信した暗号化通帳識別子を媒体秘密鍵136で復号化して通帳識別子を抽出する（S1-12）。そして、クライアント端末10は通帳識別子、銀行電子署名を電子通帳記録媒体11に記録する（S1-13）。記録が完了した場合には、クライアント端末10は、電子通帳登録システム20にインターネットIを介して記録完了通知を送信する（S1-14）。以上により、電子通帳記録媒体11の登録処理を終了する。

【0057】次に、利用者がクライアント端末10を用いて電子通帳記録媒体11に未記帳の取引明細に関するデータを記録する段階の処理を、図8～9を用いて説明する。まず、利用者は、クライアント端末10を用いてユーザ認証を行う（S2-1）。この処理は、上述したステップ（S1-1）と同様に、ユーザ認証（本人認証）と同様に行われる。具体的には、まず、利用者はクライアント端末10を用いてインターネットIを介して電子通帳登録システム20にアクセスする。次に、利用者は、電子通帳登録システム20からの要求に応じて利用者番号、銀行口座番号、暗証番号に関するデータを送

信する。データを受信した管理コンピュータ21は、受信した利用者番号、銀行口座番号、暗証番号が、銀行口座データ記憶部24に記録された銀行口座データ240と一致するかどうかを確認する。管理コンピュータ21は、一致する場合には、ユーザ認証を終了し、銀行が提供するサービスの許諾を利用者に与える。

【0058】次に、利用者は、クライアント端末10を用いて電子通帳記帳要求を行う(S2-2)。この場合、クライアント端末10は、インターネットIを介して電子通帳記帳要求を、電子通帳登録システム20に送信する。

【0059】電子通帳記帳要求を受信した管理コンピュータ21は、クライアント端末10に対して通帳識別子要求と銀行公開鍵252とを送信する(S2-3)。この場合、管理コンピュータ21は、暗号鍵データ記憶部25から銀行公開鍵252を抽出して送信する。

【0060】通帳識別子要求を受信したクライアント端末10は、利用者に対して電子通帳記録媒体11をカードリーダーライター100に挿入するように促す。具体的には、クライアント端末10のディスプレイ装置に、「電子通帳記録媒体の挿入指示」が表示される。さらに、クライアント端末10は受信した銀行公開鍵252を図示しない記憶部に記録する。次に、クライアント端末10は、電子通帳記録媒体11に記録された通帳識別子を抽出する(S2-4)。この場合、クライアント端末10はカードリーダーライター100に挿入された電子通帳記録媒体11のデータ書き込み可能領域130に記録された通帳識別子、多重ハッシュ値に関するデータを読み出す。

【0061】電子通帳記録媒体11に複数の口座識別子が記録されている場合には、それらのクライアント端末10のディスプレイ装置に表示し、利用者に電子通帳の選択を促す。そして、クライアント端末10は選択された通帳識別子の多重ハッシュ値を読み出す。なお、初めて電子通帳記録媒体11を用いて記帳する場合には、電子通帳記録媒体11には多重ハッシュ値は記録されていないので、通帳識別子のみを読み出す。次に、クライアント端末10は、読み出した通帳識別子及び多重ハッシュ値(初めて記帳する場合には通帳識別子)を暗号化して暗号化データを生成する(S2-5)。この場合の暗号化には、銀行公開鍵252を用いる。

【0062】次に、クライアント端末10は、インターネットIを介して電子通帳登録システム20に暗号化データを送信する(S2-6)。この暗号化データを受信した管理コンピュータ21は、暗号化データを復号化し、通帳識別子、多重ハッシュ値を抽出する(S2-7)。この場合、管理コンピュータ21は暗号鍵データ記憶部25に記録された銀行秘密鍵251を用いて復号化する。なお、この場合も、初めて記帳する場合には、管理コンピュータ21は通帳識別子のみを抽出する。次

に、管理コンピュータ21は復号化した通帳識別子、多重ハッシュ値の照合を行う(S2-8)。この場合、管理コンピュータ21は、この処理における銀行口座番号に関連づけられて記録された電子通帳データ230の通帳識別子、多重ハッシュ値と、復号化した通帳識別子、多重ハッシュ値とが一致するかどうかを照合する。なお、電子通帳データ230に多重ハッシュ値の記録がない場合(初めて記帳する場合)には、管理コンピュータ21は通帳識別子のみを照合する。

【0063】通帳識別子、多重ハッシュ値が一致しない場合(ステップ(S2-8)において「No」の場合)、管理コンピュータ21はインターネットIを介してクライアント端末10に取引明細データの記帳拒否を送信する(S2-9)。記帳拒否を受信したクライアント端末10のディスプレイ装置には、その旨が表示される。通帳識別子、多重ハッシュ値が一致し、認証ができた場合(「Yes」の場合)、管理コンピュータ21は未記帳明細データのハッシュ値(未記帳明細ハッシュ値)を生成する(S2-10)。ここでは、管理コンピュータ21は未記帳取引明細データ記憶部22から銀行口座番号に関連づけられた取引明細データ220を抽出し、ハッシュ関数を用いて未記帳明細ハッシュ値を算出する。そして、管理コンピュータ21は、生成したハッシュ値を電子通帳データ230の最新記帳ハッシュ値データ領域に記録する。この場合、既に最新記帳ハッシュ値データ領域にデータが記録されている場合は、算出した未記帳ハッシュ値に置き換える。

【0064】次に、管理コンピュータ21は、多重ハッシュ値を生成する(S2-11)。具体的には、まず、電子通帳データ記憶部23に記録されている多重ハッシュ値を抽出する。そして、管理コンピュータ21は、この多重ハッシュ値と未記帳明細ハッシュ値とから多重ハッシュ値を生成する。この場合、抽出した多重ハッシュ値と未記帳明細ハッシュ値とを結合し、そのデータをハッシュ関数に導入してハッシュ値を算出する。

【0065】次に、管理コンピュータ21は、算出した多重ハッシュ値を、電子通帳データ230の多重ハッシュ値データ領域に記録する(S2-12)。この場合、既に多重ハッシュ値データ領域にデータが記録されている場合は、算出した多重ハッシュ値に置き換える。

【0066】次に、管理コンピュータ21は、未記帳明細データ、未記帳明細ハッシュ値を媒体識別子で暗号化する(S2-13)。この場合、まず、管理コンピュータ21は電子通帳データ記憶部23に記録された媒体識別子を抽出する。次に、管理コンピュータ21は、抽出した媒体識別子を用いて、未記帳明細データ、未記帳明細ハッシュ値を個別に暗号化することにより、暗号化取引明細データ、暗号化ハッシュ値を生成する。

【0067】次に、管理コンピュータ21は、インターネットIを介して暗号化したデータをクライアント端末

10に送信する(S2-14)。クライアント端末10は、電子通帳記録媒体11に受信したデータを記録する(S2-15)。この場合、クライアント端末10は、受信したデータを通帳識別子に関連づけて暗号化データ134として電子通帳記録媒体11に追加記録する。

【0068】次に、クライアント端末10は受信したデータの復号化を行う(S2-16)。ここでは、まず、クライアント端末10は電子通帳記録媒体11に記録された媒体識別子121を抽出する。次に、クライアント端末10は、媒体識別子121を用い、受信した暗号化取引明細データ、暗号化ハッシュ値を復号化し、未記帳明細データ、未記帳明細ハッシュ値を抽出する。

【0069】次に、クライアント端末10は、抽出した未記帳明細データと未記帳明細ハッシュ値とを照合する(S2-17)。具体的には、クライアント端末10は、ハッシュ関数を用いて未記帳明細データのハッシュ値を算出し、抽出した未記帳明細ハッシュ値と算出したハッシュ値とが一致するかどうかを確認する。抽出した未記帳明細ハッシュ値と算出したハッシュ値とが一致しない場合、クライアント端末10はエラーを出力し、処理を終了する。

【0070】抽出した未記帳明細ハッシュ値と算出したハッシュ値とが一致する場合、クライアント端末10は、多重ハッシュ値を生成する(S2-18)。具体的には、まず、クライアント端末10は電子通帳記録媒体11に記録されている多重ハッシュ値を抽出する。そして、クライアント端末10は、この多重ハッシュ値と未記帳明細ハッシュ値とから多重ハッシュ値を生成する。この場合、抽出した多重ハッシュ値と未記帳明細ハッシュ値とを結合し、そのデータをハッシュ関数に導入してハッシュ値を算出する。そして、クライアント端末10は、算出した多重ハッシュ値を、通帳識別子と関連づけて多重ハッシュ値データ135の多重ハッシュ値データ領域に記録する。この場合、既に多重ハッシュ値データ領域にデータが記録されている場合は、算出した多重ハッシュ値に置き換える。そして、クライアント端末10はインターネットIを介して電子通帳登録システム20に記録完了の通知する(S2-19)。記録完了通知を受信した管理コンピュータ21は、この未記帳取引明細データ記憶部22に記録された取引明細データ220を消去する。以上により、電子通帳記録媒体11への取引明細データの記録処理を終了する。

【0071】次に、利用者が、クライアント端末10を用いて取引明細を表示する段階の処理を、図10を用いて説明する。まず、利用者は、クライアント端末10を用いて電子通帳の表示要求を入力する(S3-1)。この場合、クライアント端末10は利用者に対して、電子通帳記録媒体11をカードリーダーライター100に挿入するように促す。次に、クライアント端末10は、電子通帳記録媒体11に記録されているすべての通帳識別

子を抽出する(S3-2)。

【0072】次に、クライアント端末10は抽出した通帳識別子をディスプレイ装置に表示して、利用者に対して通帳識別子の選択を促す(S3-3)。通帳識別子が選択された場合には、クライアント端末10は、データ書込み不可領域120に記録された媒体識別子121、及び選択された通帳識別子に関連づけられて記録された暗号化データ134を抽出する(S3-4)。次に、クライアント端末10は抽出した媒体識別子121で暗号化データ134の暗号化取引明細データ、暗号化ハッシュ値を復号化する(S3-5)。

【0073】次に、取引明細データに関してハッシュ値の検証する(S3-6)。この場合、クライアント端末10は取引明細データをハッシュ関数に導入し、ハッシュ値を算出し、抽出したハッシュ値と比較する。両者が不一致の場合は、取引明細の表示を拒否する(S3-7)。両者が一致する場合は、クライアント端末10は取引明細を表示する(S3-8)。以上により、取引明細の表示処理を終了する。

【0074】以上、本実施形態によれば、以下に示す効果を得ることができる。

- ・ 上記実施形態では、電子通帳記録媒体11として、媒体識別子121の記録されたデータ書込み不可領域120を有する記録媒体を用いる。このような記録媒体は市販されているので、利用者のハードウェア、通信等の環境や好み等に応じて、取引明細データを記録する媒体を選択して通帳を作成することができる。さらに、媒体識別子121はデータ書込み不可領域120に記録されているので、電子通帳の複製など偽造を防止できる。

- ・ 【0075】上記実施形態では、電子通帳記録媒体11には暗号化された取引明細に関するデータが記録されている。このため、このデータを媒体識別子121で復号化すれば、取引明細データをクライアント端末10に電子的に取り込むことが可能である。従って、この取引明細データを家計簿等に容易に加工できる。

- ・ 【0076】上記実施形態では、電子通帳記録媒体11には、通帳識別子データ133が記録されている。このため、銀行の預金通帳としての電子通帳記録媒体11を客観的に認証できる。

- ・ 【0077】上記実施形態では、電子通帳記録媒体11には、通帳識別子データ133と銀行署名データとが関連づけられて記録されている。この通帳識別子は、媒体識別子121に基づいて生成されるため、電子通帳記録媒体11に記録された取引明細データを複製し、真正な電子通帳記録媒体11以外への記録を防止できる。さらに、この通帳識別子には、銀行口座識別子に関する情報を含んでいるので、電子通帳記録媒体11に複数の銀行口座に関する銀行署名データを記録させることができる。

- ・ 【0078】上記実施形態では、暗号化データ13

4には、暗号化取引明細データと暗号化ハッシュ値とに関するデータとが、通帳識別子に関連づけられて記録されている。このため、複数の銀行口座に対して通帳識別子毎に取引明細データを電子通帳記録媒体11に記録することができる。従って、従来のように銀行口座毎に通帳を持つ必要がなく、通帳管理の自由度を大きくすることができる。

【0079】・ 上記実施形態では、暗号化データ134には、暗号化取引明細データと暗号化ハッシュ値とに関するデータとが、通帳識別子に関連づけられて記録されている。この暗号化取引明細データと暗号化ハッシュ値は、媒体識別子121を用いて暗号化されている。暗号化取引明細データと暗号化ハッシュ値とを他の電子通帳記録媒体11に記録した場合、媒体識別子121が異なるので、暗号化取引明細データを正確に復号化できない。さらに、取引明細データとそのハッシュ値が不一致になるので、取引明細が表示されない。従って、取引明細データの複製、真正な電子通帳記録媒体11以外への記録を防止できる。

【0080】・ 上記実施形態では、暗号化データ134には、暗号化取引明細データと暗号化ハッシュ値とに関するデータとが関連づけられて記録されている。このため、ハッシュ関数を用いることにより、データの真正性を容易に検証することができる。

【0081】・ 上記実施形態では、多重ハッシュ値データ135には、多重ハッシュ値に関するデータが、通帳識別子に関連づけられて記録されている。この多重ハッシュ値は、過去の取引明細に関する情報を含むため、一部の取引明細データを削除、追加、改変した場合にも、多重ハッシュ値の相違から、偽造、改変を確実に把握できる。

【0082】・ 上記実施形態では、電子通帳データ記憶部23には、図4に示すように、利用者が使用する電子通帳に関する電子通帳データ230が記録される。そして、電子通帳データ230には、媒体識別子、通帳識別子、媒体公開鍵、最新記帳ハッシュ値、多重ハッシュ値に関するデータが、銀行口座番号に関するデータと関連づけられて記録される。このため、銀行が認めた電子通帳記録媒体11を確実に特定できる。

【0083】・ 上記実施形態では、管理コンピュータ21は、未記帳明細データ、未記帳明細ハッシュ値を暗号化し、クライアント端末10に送信する。この暗号化には媒体識別子121が用いた共通鍵暗号方式を用いる。このため、守秘性を担保した暗号化が容易にでき、管理コンピュータ21、クライアント端末10の暗号化、復号化の負荷を軽減できる。

【0084】なお、上記実施形態は、以下の態様に変更してもよい。

・ 上記実施形態では、通帳識別子を銀行秘密鍵251で暗号化して銀行署名データを生成した。これに代え

て、媒体識別子121のみを銀行秘密鍵251で暗号化して銀行署名データを生成してもよい。この場合、電子通帳記録媒体11に記録する電子通帳は一つの銀行口座とする。これにより、媒体識別子121に基づいて生成された銀行署名データであれば、通帳としての電子通帳記録媒体11を客観的に認証できる。

【0085】・ 上記実施形態では、ステップ(S2-3)において、管理コンピュータ21はクライアント端末10に対して通帳識別子要求と銀行公開鍵252とを送信した。これに代えて、媒体識別子121を要求してもよい。この場合、電子通帳記録媒体11に記録する電子通帳は一つの銀行口座とする。これにより、媒体識別子121に基づいて電子通帳記録媒体11を認証できる。

【0086】・ 上記実施形態では、管理コンピュータ21やクライアント端末10は、銀行公開鍵や媒体公開鍵を、相手方に送信した。これに代えて、必要に応じて認証登録証明機関のシステムから公開された鍵を取得してもよい。これにより、電子通帳データ記憶部23に媒体公開鍵を記録する必要がなくなる。

【0087】・ 上記実施形態では、管理コンピュータ21は、通帳記帳の際には、通帳識別子、多重ハッシュ値を用いて、電子通帳記録媒体11の真正性を確認した。これに代えて、暗号化データ134の暗号化ハッシュ値を用いて真正性を確認してもよい。この場合には、図11～12に示す手順を用いる。上記実施形態と同様に、クライアント端末10と電子通帳登録システム20との間でユーザ認証を行う(S4-1)。次に、クライアント端末10は電子通帳記帳要求を送信し(S4-2)、管理コンピュータ21は通帳識別子要求、銀行公開鍵を送信する(S4-3)。ここで、クライアント端末10は、通帳識別子、最後に記録された暗号化ハッシュ値を抽出する(S4-4)。そして、通帳識別子、抽出した暗号化ハッシュ値を銀行公開鍵で暗号化し(S4-5)、このデータを電子通帳登録システム20に送信する(S4-6)。

【0088】管理コンピュータ21は、受信したデータを銀行秘密鍵で復号化して通帳識別子、暗号化ハッシュ値を抽出する(S4-7)。さらに、暗号化ハッシュ値を媒体識別子で復号化してハッシュ値を抽出する(S4-8)。次に、管理コンピュータ21は、抽出したハッシュ値と電子通帳データ記憶部23に記録された最新記帳ハッシュ値との照合を行う(S4-9)。両者が一致しない場合は、管理コンピュータ21はクライアント端末10に記帳拒否を通知する(S4-10)。両者が一致する場合は、管理コンピュータ21は、未記帳明細データのハッシュ値を生成する(S4-11)。そして、未記帳明細データ、未記帳明細ハッシュ値を媒体識別子で暗号化し、クライアント端末10に送信する(S4-12)。

【0089】クライアント端末10は、受信したデータを電子通帳記録媒体11に記録する（S4-13）。この場合、上記実施形態と同様に、クライアント端末10は、暗号化未記帳明細データを暗号化取引明細データとして、暗号化未記帳明細ハッシュ値を暗号化ハッシュ値として記録する。さらに、クライアント端末10は、受信したデータを復号化する（S4-14）。そして、未記帳明細データと未記帳明細ハッシュ値とを比較し、照合する（S4-15）。次に、クライアント端末10は、電子通帳記録媒体11に記録された多重ハッシュ値を抽出する（S4-16）。そして、電子通帳記録媒体11に記録されていた多重ハッシュ値及び未記帳明細ハッシュ値から、新しい多重ハッシュ値を生成し（S4-17）、電子通帳記録媒体11に多重ハッシュ値として上書き記録する（S4-18）。その後、クライアント端末10は、電子通帳登録システム20に記録完了の通知を行う（S4-19）。この場合、電子通帳データ記憶部23に多重ハッシュ値を記録しておく必要がなく、電子通帳データ記憶部23に記憶容量を削減できる。

【0090】・ 上記実施形態では、多重ハッシュ値は、過去の多重ハッシュ値と未記帳明細データのハッシュ値とを用いて生成した。これに代えて、最初の多重ハッシュ値は通帳識別子から生成してもよい。これにより、電子通帳記録媒体11の真正性と取引明細データの真正性とを、より確実に担保できる。

【0091】・ 上記実施形態では、ステップ（S3-4）において、通帳識別子が選択された場合には、クライアント端末10は、データ書込み不可領域120に記録された媒体識別子121及び選択された通帳識別子に関連づけられて記録された暗号化データ134を抽出した。これに代えて、表示させる取引明細の範囲を指定させてもよい。この場合、まず、クライアント端末10は利用者に、表示させる取引明細の範囲の入力を促す。そして、クライアント端末10は暗号化データ134を抽出し、指定された範囲の取引明細データに関するハッシュ値のみを抽出し、ステップ（S3-5）～（S3-8）を実行する。これにより、クライアント端末10の負荷を軽減しながら、利用者が所望の取引明細のみを表示することができる。

【0092】・ 上記実施形態では、ステップ（S2-15）において、クライアント端末10が、受信したデータを通帳識別子に関連づけて暗号化データ134として電子通帳記録媒体11に記録した。これに代えて、クライアント端末10は受信したデータをそのまま電子通帳記録媒体11に記録してもよい。この場合は、管理コンピュータ21が、暗号化したデータに通帳識別子に関連づけて送信する。これにより、クライアント端末10の処理を削減できる。

【0093】・ 上記実施形態では、ステップ（S2-17）において、抽出した未記帳明細ハッシュ値と算出

したハッシュ値とが一致しない場合、クライアント端末10はエラーを出力し、処理を終了した。これに加え、クライアント端末10が管理コンピュータ21にエラーのあったことを送信してもよい。この場合、管理コンピュータ21は元の未記帳ハッシュ値、多重ハッシュ値を仮記憶しておき、クライアント端末10からエラーを受信した場合には、未記帳ハッシュ値、多重ハッシュ値を元の値に戻す。これにより、エラー時にもデータを維持でき、正確な記帳が可能である。

【0094】・ 上記実施形態では、一つの銀行口座に対して一つの電子通帳記録媒体11を用いたが、途中で電子通帳記録媒体11を変更させてもよい。この場合、図7に示す電子通帳記録媒体11の登録処理を再度行う。その場合、管理コンピュータ21は、電子通帳データ記憶部23に記録された媒体識別子、通帳識別子、媒体公開鍵を、新しい電子通帳記録媒体11にあわせて変更する。これにより、電子通帳記録媒体11のデータ書込み可能領域130が飽和した場合や利用者が新しい電子通帳記録媒体11に取引明細データを記録する場合にも対応できる。

【0095】・ 上記実施形態では、電子通帳記録媒体11に記録する取引明細データ、ハッシュ値は媒体識別子121で暗号化した。暗号化に用いる鍵は媒体識別子そのものを使用する必要はなく、これに代えて、通帳識別子で暗号化してもよい。通帳識別子は、媒体識別子121と銀行口座に関するデータとから生成されるため、銀行口座に関する情報に関連づけた暗号化を実現できる。

【0096】・ 上記実施形態では、クライアント端末10／電子通帳登録システム20間をインターネットIで接続した。この代わりに、専用線や公衆回線を用いて接続してもよい。この場合、仮想的な専用線であってもよい。これにより、より安全に取引を行うことができる。

【0097】・ 上記実施形態では、電子通帳登録システム20に、各記憶部（22～25）を設けたが、他のシステムの記憶部を利用してもよい。例えば、銀行口座データ記憶部24は、銀行が有する他のシステムに設置してもよい。これにより、既存の銀行口座に関するデータを利用できる。

【0098】・ 上記実施形態では、取引明細を表示する端末としてクライアント端末10を用いた。これに代えて、電子通帳記録媒体11に記録されたデータを読み込むことができる携帯電話端末やPDA（Personal Digital Assistant）を用いてもよい。また、クライアント端末10として双方向テレビジョン端末を用いてもよい。この場合、電子通帳登録システム20から利用者に向けて情報を流す下りチャンネルと、利用者から電子通帳登録システム20にデータを送る上りチャンネルとを準備する。これにより、色々な端末を用いて、取引明細を表

示させることができる。

【0099】・ 上記実施形態では、電子通帳記録媒体11として、記録媒体を用いた。これに代えて、データ書き込み不可領域120が設定された記憶端末を用いてもよい。この場合も、データ書き込み不可領域120には、その端末を特定する識別子を事前に記録しておく。これにより、記録媒体の自由度を確保することができる。

【0100】

【発明の効果】 以上詳述したように、本発明によれば、金融機関における取引明細データを記録媒体に記録させることができるので、利用者にとって迅速に取引明細を取得できる。また、取引明細データの加工も容易である。一方、金融機関にとっても、真正性を担保した電子通帳を利用者に提供できる。

【図面の簡単な説明】

【図1】 本発明の実施形態のシステム概略図。

【図2】 電子通帳記録媒体に記録されたデータの説明図。

【図3】 未記帳取引明細データ記憶部に記録されたデータの説明図。

【図4】 電子通帳データ記憶部に記録されたデータの説明図。

【図5】 銀行口座データ記憶部に記録されたデータの説明図。

【図6】 暗号鍵データ記憶部に記録されたデータの説明図。

【図7】 本実施形態の処理手順の説明図。

【図8】 本実施形態の処理手順の説明図。

【図9】 本実施形態の処理手順の説明図。

【図10】 本実施形態の処理手順の説明図。

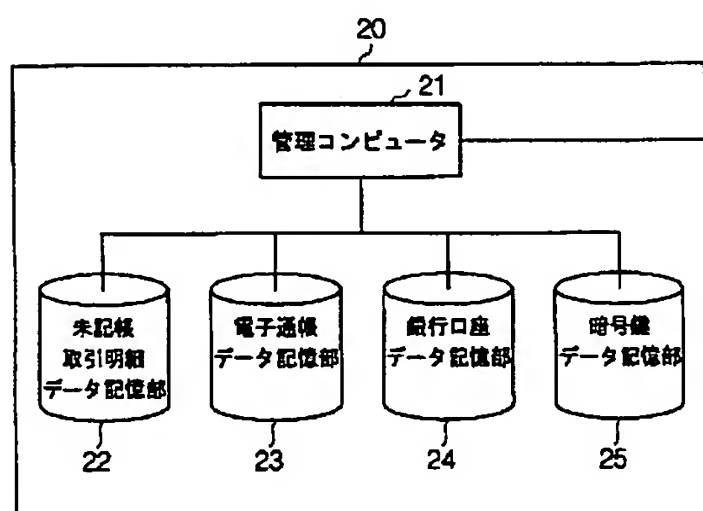
【図11】 他の実施形態の処理手順の説明図。

【図12】 他の実施形態の処理手順の説明図。

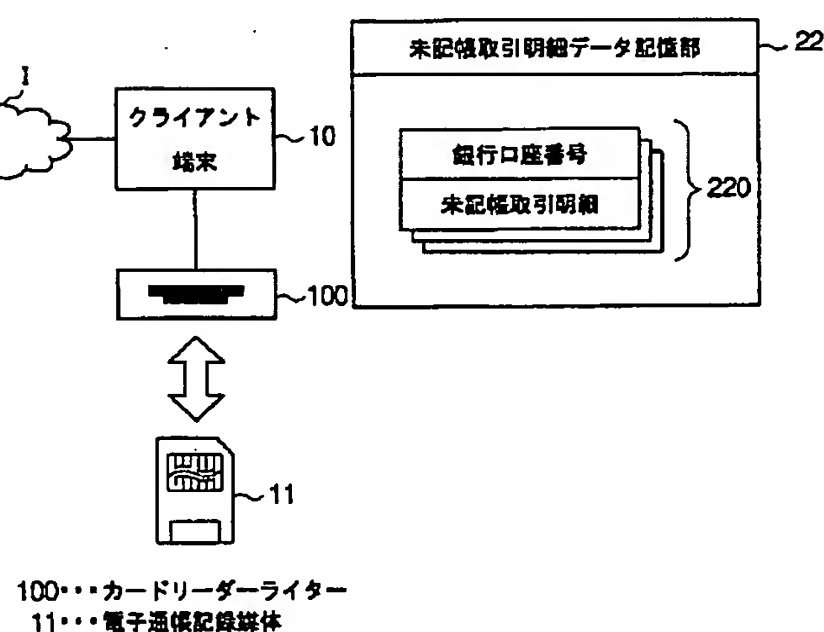
【符号の説明】

10…クライアント端末、11…電子通帳記録媒体、120…データ書き込み不可領域、20…電子通帳登録システム、21…管理コンピュータ、23…電子通帳データ記憶手段としての電子通帳データ記憶部、24…銀行口座データ記憶手段としての銀行口座データ記憶部、25…暗号鍵データ記憶手段としての暗号鍵データ記憶部、I…インターネット。

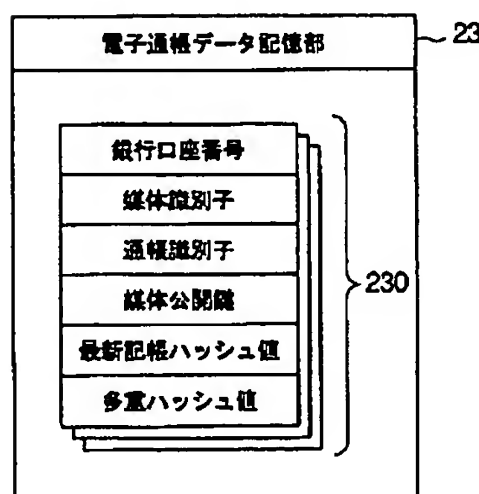
【図1】



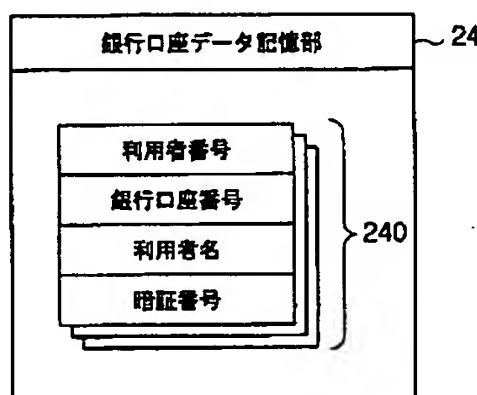
【図3】



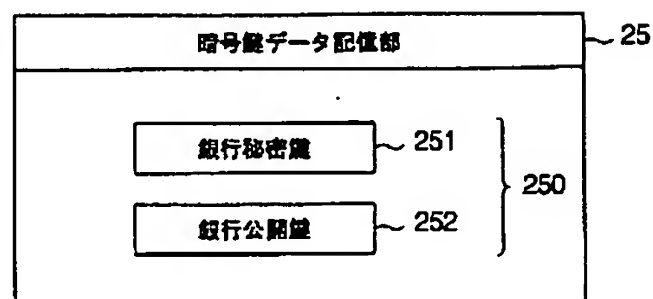
【図4】



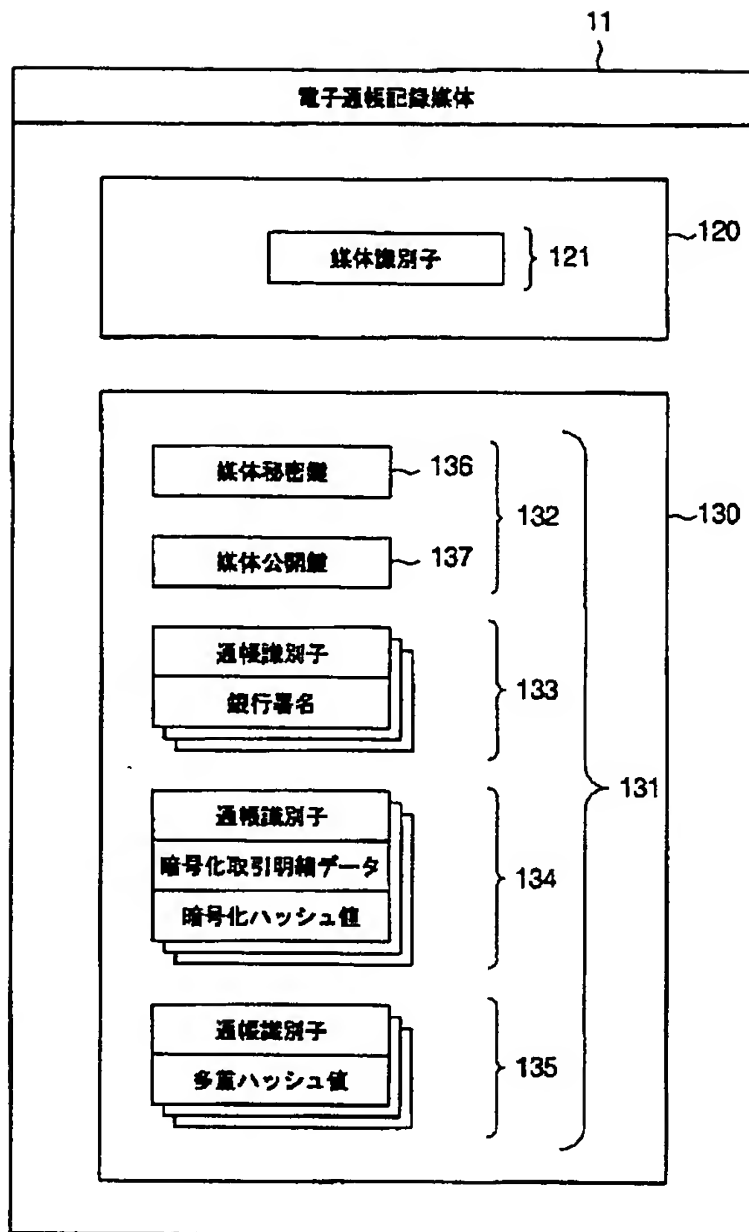
【図5】



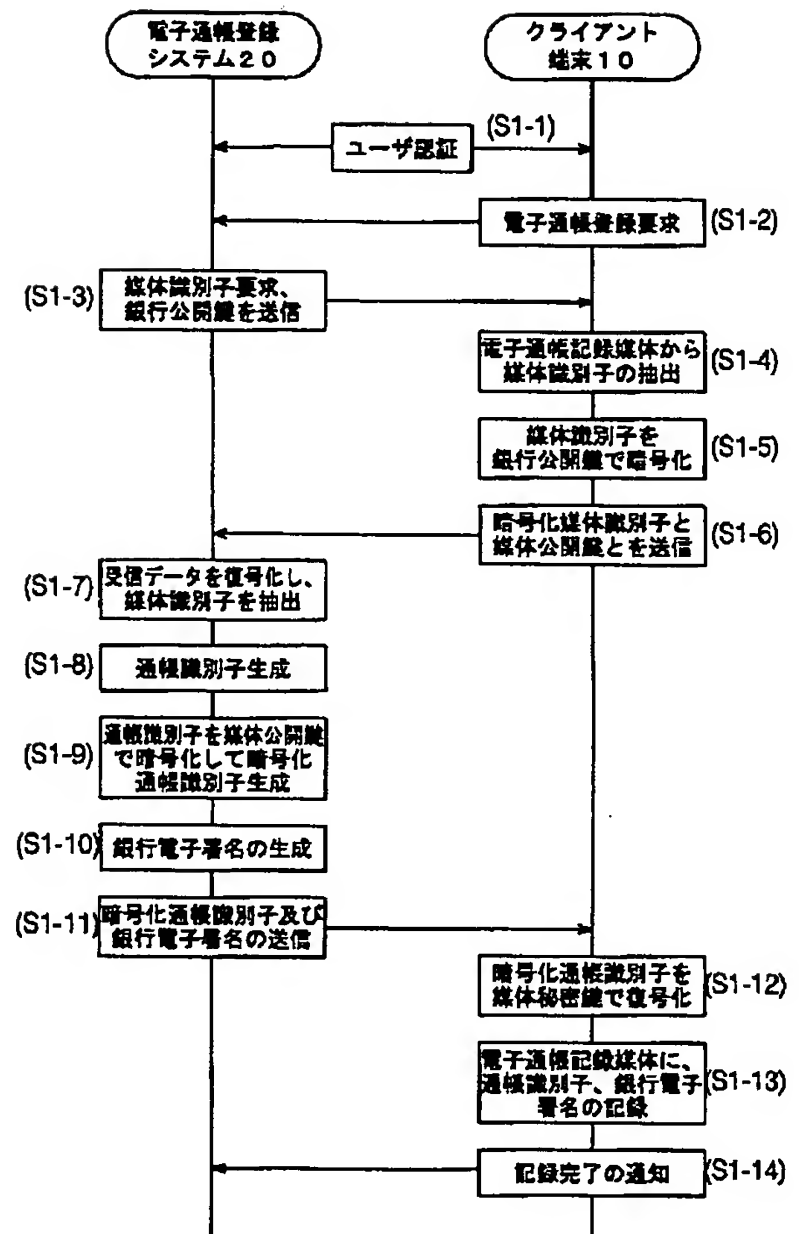
【図6】



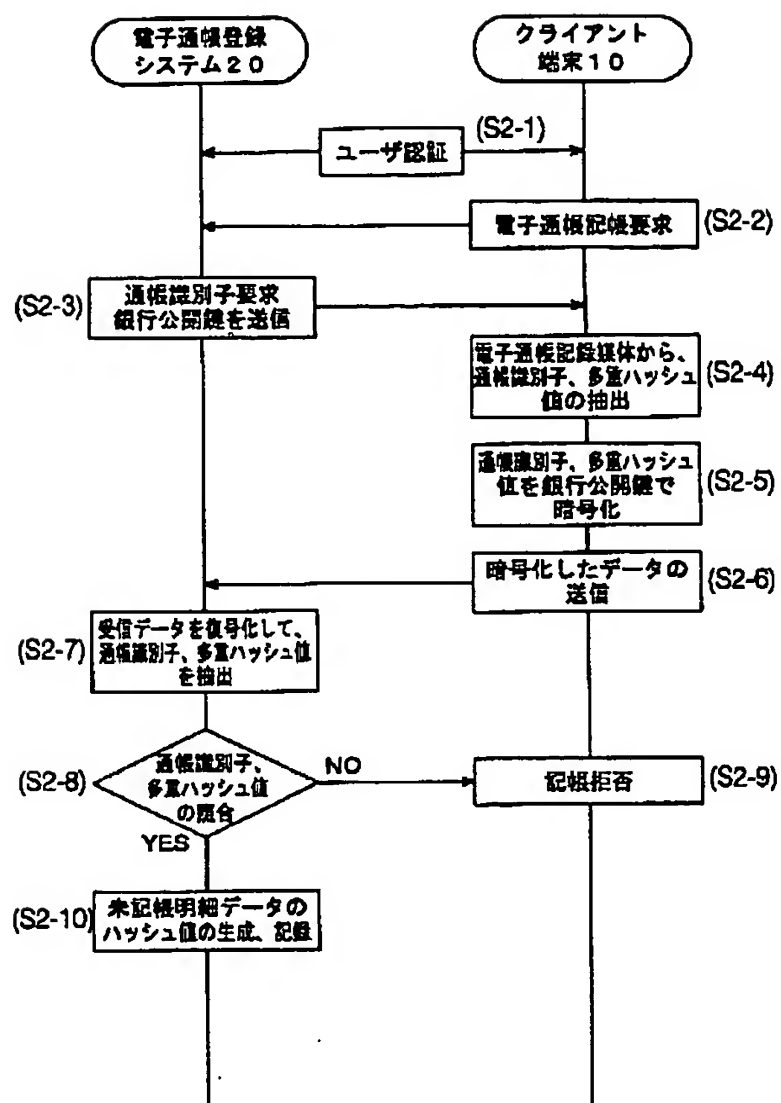
【図 2】



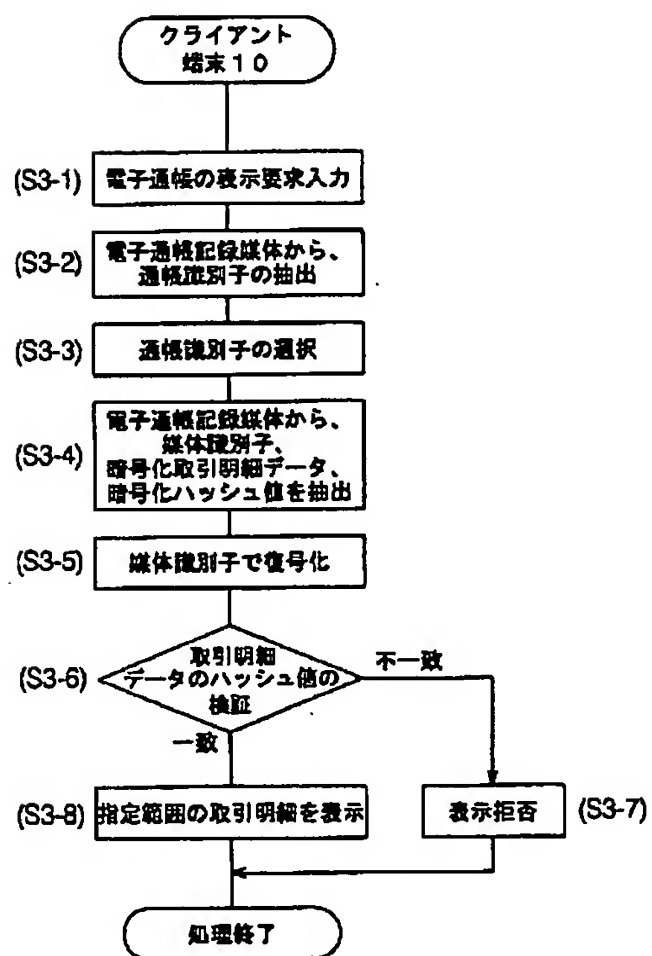
【図 7】



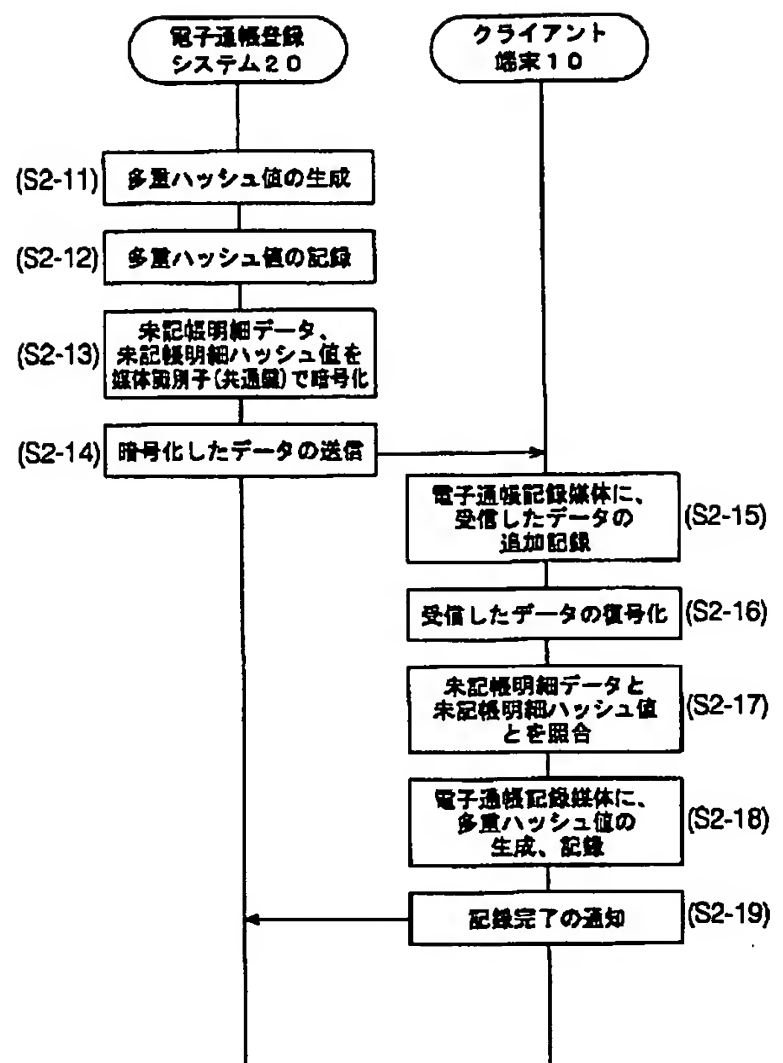
【図 8】



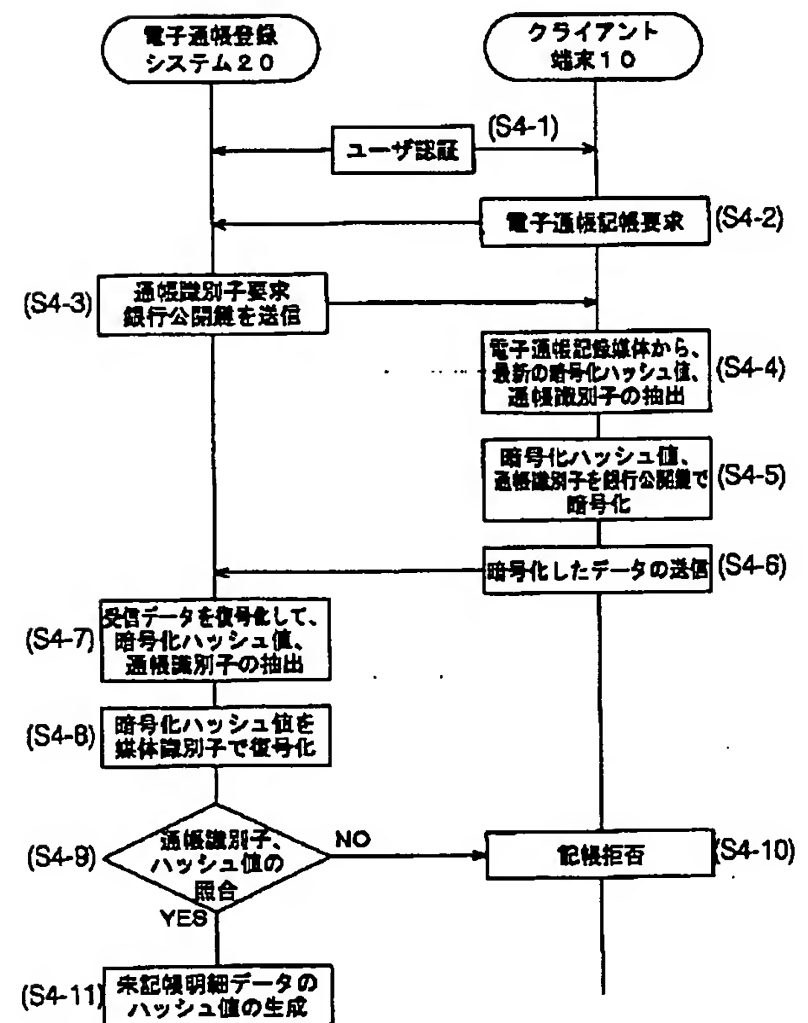
【図 10】



【図 9】



【図 11】



【図12】

